Claims

What I claim as my invention is:

1. A personal computer system for maintaining a digital data file, comprising:

a personal computer having installed therein a trusted time source;

means for saving the file at a moment in time;

means for retrieving from said trusted time source a date and a time corresponding to said moment in time;

means for appending said date and said time retrieved from said trusted time source to said saved file;

means for signing said saved file with said date and said time retrieved from said trusted time source appended thereto;

means for hashing said signed file to produce a digest;

means for signing said digest with a key to produce a certificate;

means for appending said certificate to said saved file; and

means for saving said file with said certificate appended thereto.

2. The personal computer system according to claim 1, further comprising means for verifying the authenticity of said file with said certificate appended thereto.

3. The personal computer system according to claim 2, wherein said verification means comprises means for signing said saved file with said date and said time retrieved from said trusted time source appended thereto with an ID.

4. The personal computer system according to claim 3, wherein said ID is selected from the group consisting of an ID corresponding to a user, an ID corresponding to a system used by said user, and an ID corresponding to an enterprise within which said user uses the personal computer system.

5. The personal computer system according to claim 4, wherein said user ID is selected from the group consisting of a plurality of characters identifying said user, first data representing an iris scan of said user, second data representing a retina scan of said user, third data representing a finger scan of said user, fourth data representing said user's hand geometry, fifth data representing said user's voice, sixth data representing said user's signature, and combinations of said plurality of characters, first, second, third, fourth, fifth, and sixth data.

6. The personal computer system according to claim 1, wherein said trusted time source comprises:

a real time clock; and

a battery coupled to and powering said real time clock.

7. The personal computer system according to claim 6, wherein said real time clock and said battery are installed on a motherboard of said personal computer.

8. The personal computer system according to claim 6, wherein said real time clock and said battery are installed on a baseboard of said personal computer.

9. The personal computer system according to claim 6, wherein said real time clock and said battery are installed on an expansion card adapted to be coupled to a motherboard of said personal computer.

10. The personal computer system according to claim 6, wherein said real time clock and said battery are installed on an expansion card adapted to be coupled to a baseboard of said personal computer.

11. The personal computer system according to claim 6, wherein said real time clock and said battery are installed on an external device adapted to be coupled to said personal computer.

12. The personal computer system according to claim 11, wherein said external device comprises a dongle.

13. The personal computer system according to claim 11, wherein said external device comprises a PCMCIA card.

14. The personal computer system according to claim 11, wherein said external device comprises a smart card.

15. The personal computer system according to claim 11, wherein said external device comprises a removable computer-readable medium.

16. The personal computer system according to claim 15, wherein said removable computer-readable medium is selected from the group consisting of a magnetic hard disk, a floppy disk, an optical disk, a CD-ROM, a CD-R, a CD-RW, a disk compliant with DVD standards, a magneto-optical disk, a magnetic tape, a memory chip, a carrier wave used to carry computer-readable electronic data, such as are used in transmitting and receiving an e-mail or in accessing a network, including the Internet, intranets, extranets, virtual private networks (VPN), local area networks (LAN), and wide area networks (WAN), and any other storage device used for storing data accessible by a computer.

17. A method of maintaining a digital data file in a personal computer, comprising:

providing a trusted time source in the personal computer;

saving the file at a moment in time;

retrieving from said trusted time source a date and a time corresponding to said moment in time;

appending said date and said time retrieved from said trusted time source to said saved file;

signing said saved file with said date and said time retrieved from said trusted time source appended thereto;

hashing said signed file to produce a digest;

signing said digest with a key to produce a certificate;

appending said certificate to said saved file; and

saving said file with said certificate appended thereto.

18. The method according to claim 17, further comprising the step of providing tamper-evident means for labeling said trusted time source.

19. The method according to claim 17, wherein said moment in time corresponds to an access of the digital data file.

20. The method according to claim 17, wherein said moment in time corresponds to a creation of the digital data file.

21. The method according to claim 17, wherein said moment in time corresponds to a modification of the digital data file.

22. The method according to claim 17, wherein said moment in time corresponds to a receipt of the digital data file.

23. The method according to claim 17, wherein said moment in time corresponds to a transmission of the digital data file.

24. The method according to claim 17, further comprising the steps of:

appending to an e-mail said saved file with said certificate appended thereto;

transmitting said e-mail, with said appended saved file having said certificate appended thereto, to a remote computer;

determining a first delay time associated with said transmission step;

adding said first delay time to said moment in time to provide a first relative trusted time at which said e-mail was received by said remote computer; and

storing said first relative trusted time in the personal computer.

25. The method according to claim 24, further comprising the step of appending a request for return receipt of a message indicating a remote time at which said e-mail was opened at said remote computer.

26. The method according to claim 25, wherein said e-mail has been opened at said remote computer at said remote time, thereby, transmitting said message, further comprising the steps of:

receiving, at the personal computer at another moment in time, said message from said remote computer;

determining a second delay time associated with the transmission of said message;

retrieving from said trusted time source a date and a time corresponding to said other moment in time;

subtracting said second delay time from said other moment in time to provide a second relative trusted time at which said message was received by the personal computer; and

storing said second relative trusted time in the personal computer.

27. The method according to claim 26, further comprising the steps of:

determining a differential between said second relative trusted time stored in the personal computer and said remote time;

storing said differential in the personal computer; and

thereafter using said stored differential to approximate third and subsequent relative trusted times in communications with the remote computer.

28. The method according to claim 17, further comprising another digital data file and further comprising the steps of:

saving said other file at a second moment in time;

retrieving from said trusted time source a date and a time corresponding to said second moment in time;

appending said date and said time retrieved from said trusted time source to said other saved file;

signing said other saved file with said date and said time retrieved from said trusted time source appended thereto;

hashing said signed other file to produce another digest;

signing said other digest with a key to produce another certificate;

appending said other certificate to said other saved file;

saving said other file with said other certificate appended thereto; and

appending said file with said certificate appended thereto to said other file with said other certificate appended thereto.

29. A method of maintaining a first digital data file and a second digital data file in a personal computer, comprising:

providing a trusted time source in the personal computer;

saving the first digital data file at a first moment in time;

retrieving from said trusted time source a date and a time corresponding to said first moment in time;

appending said date and said time retrieved from said trusted time source to said first saved file;

signing said first saved file with said date and said time retrieved from said trusted time source appended thereto;

hashing said signed first file to produce a first digest;

signing said first digest with a key to produce a first certificate;

appending said first certificate to said first saved file; and

saving said first saved file with said first certificate appended thereto.

30. The method according to claim 29, further comprising the step of appending said first saved file, with said first certificate appended thereto, to the second digital data file.

31. The method according to claim 30, further comprising the steps of:

saving the second digital data file at a second moment in time;

retrieving from said trusted time source a date and a time corresponding to said second moment in time;

appending said date and said time retrieved from said trusted time source to said second saved file;

signing said second saved file with said date and said time retrieved from said trusted time source appended thereto;

hashing said signed second file to produce a second digest;

signing said second digest with a key to produce a second certificate;

appending said second certificate to said second saved file; and

saving said second saved file with said second certificate appended thereto.

32. The method according to claim 30, further comprising the steps of:

saving a combination of said first saved file with said first certificate appended thereto and the second digital data file at a second moment in time;

retrieving from said trusted time source a date and a time corresponding to said second moment in time;

appending said date and said time retrieved from said trusted time source to said combination;

signing said combination with said date and said time retrieved from said trusted time source appended thereto;

hashing said signed combination to produce a third digest;

signing said third digest with a key to produce a third certificate;

appending said third certificate to said combination; and

saving said combination with said third certificate appended thereto.

33. The method according to claim 30, wherein the first saved file comprises an e-mail and the second saved file comprises a document selected from the group consisting of a word processing document, a spreadsheet document, a database document, an HTML document, a Web page, and an image.

34. The method according to claim 33, further comprising the step of transmitting said e-mail with said document appended thereto.

35. The method according to claim 29, wherein the first saved file comprises a document selected from the group consisting of an e-mail, a word processing document, a spreadsheet document, a database document, an HTML document, a Web page, and an image.